REMARKS

I. INTRODUCTION

This amendment is being submitted under Rule 116 to place the application in condition for allowance or at least in improved condition for appeal. Accordingly, applicant respectfully requests the Examiner to enter the proposed amendment.

Applicant submitted to the Examiner in May, 2005 a draft of a proposed amendment under Rule 116 with the understanding that the draft was being submitted on an informal basis without being filed in the USPTO. The Examiner and applicant's attorney discussed the proposed amendment by telephone on Thursday, June 9, 2005. On the basis of this discussion, applicant has revised a number of the claims in the draft of May, 2005 and has revised the discussion in the REMARKS to reflect the changes in the claims. Also, in accordance with this discussion, applicant has limited the claims to claims 115-121, 145-150, 159-183, 187-191 and 226-242. Applicant respectfully submits that the claims now in the application are definite and are consistent with the corresponding claims in the previous amendment and with the claims as originally filed.

Applicant has proposed amendments in a number of the claims. These amendments have not affected the scope of the claims or the combinations recited in the claims. The amendments have been provided to clarify language previously in the claims. Applicant respectfully submits that the clarifying language in the claims provides the same meaning, and the same scope of protection, as the language that it replaces in

the claims. In view of this, applicant respectfully submits that the Examiner should enter the proposed amendment.

Applicant has eliminated such terminology in the claims as "encrypted" and "without encrypting the unencrypted message." Applicant has eliminated such language from the claims in order to avoid alleged problems which the Examiner has expressed in the use of such language. According to the Examiner, these alleged problems arise under 35 U.S.C. §112, paragraph 1. As will be seen from the subsequent discussion, these alleged problems actually do not exist since an unencrypted message is the same as a message (as distinguished from an encrypted message). Even though applicant should not have to amend the claims because a message is the same as an unencrypted message, applicant has amended the claims to eliminate the terms "unencrypted" and "without encrypting the unencrypted message" so that any alleged problems indicated by the Examiner under 35 U.S.C. §112, paragraph 1, will vanish.

In view of the above, applicant respectfully requests the Examiner to enter the proposed amendment.

II. REJECTION BY THE EXAMINER OF CLAIMS UNDER 35 U.S.C. § 112, FIRST PARAGRAPH

Claims 115-121, 145-150, 159-183, 187-191 and 226-242 have been retained in the application, all of them in at least somewhat amended form. The claims have been amended to clarify the language in the claims without affecting the scope of the claims. As now written, the claims are believed to be definite, to meet the requirement of 35

U.S.C. § 112, first paragraph and to be allowable over the references cited by the Examiner whether the references are used individually or in combination. Furthermore, the scope of claims 115-121, 145-150, 159-183, 187-191 and 226-242 in this amendment corresponds to the scope of the claims in the previous amendment and to the scope of the claims as originally filed.

The Examiner has rejected the claims under 35 U.S.C. § 112, first paragraph. According to the Examiner, applicant has not disclosed the specification sufficiently clearly for one of ordinary skill in the art to recognize the steps in the claims (as filed in the previous amendment) where applicant recites that the message is unencrypted. However, the word "unencrypted" is passive. Furthermore, the word "unencrypted" is the opposite of "encrypted." Applicant has described "encryption" in the specification in explaining how a digital signature of a message is formed. Furthermore, Barkan has described that a message is encrypted. This indicates that the message is unencrypted before it is "encrypted."

Applicant's specification and Barkan's specification provide support for applicant's recitation in the claims of an unencrypted message. Furthermore, a person of ordinary skill in the art would understand what an "unencrypted" message is. An unencrypted message is in the form in which the message is provided. The message does not have to be changed in any way in order to be unencrypted. An "unencrypted message" recited in a claim provides the same meaning as the word "message" recited in the claim without the inclusion of the word "unencrypted.".

The Examiner has indicated that there is a contradiction because applicant has recited a "digital signature" of a message and a "digital signature" includes an encryption. However, the digital signature of the message is different from the message. It is in addition to the message. The claims have been amended to indicate that the digital signature of the message is in addition to the message. Applicant believes that he has made this distinction in the language of the claims. This indicates that the message is maintained without any encryption and that the digital signature is in addition to the message. Applicant believes that the language now used in the claims should eliminate any confusion of the Examiner between the "message" and the "digital signature of the message."

The Examiner has also rejected the claims under 35 U.S.C. § 112, first paragraph on page 4 of the Office Action dated March 18, 2004, on the ground that the claims contain "subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention." Applicant respectfully disagrees with the Examiner. A person of ordinary skill in the art would instantly appreciate that a user of applicant's system would not have to do anything to a message to make the message unencrypted. Furthermore, applicant respectfully submits that applicant's specification makes it quite clear that a "message" in this application (as the term is used in the specification or in the claims) is unencrypted.

The Examiner has also rejected the claims on the grounds that the inclusion of the word "unencrypted" in the claims would require "undue experimentation" beyond the

experimentation of one of ordinary skill in the art to practice the steps which include the word "unencrypted" or "without any encryption." Applicant respectfully disagrees with the Examiner. If the message has no encryption, it does not have to be changed. If the message is not changed, it does not require any experimentation.

A message is either encrypted or unencrypted. If applicant's message were encrypted, the recipient at the destination address would have to know how to decrypt the encrypted message in order to be able to read the message. Applicant would have to furnish the decryption code to the recipient at the destination address in order for the recipient to decrypt the encrypted message. Applicant has not provided a decryption code to the recipient in this application. This indicates that applicant intended the message to be unencrypted so that, when used in the claims, the word "unencrypted" in the term "unencrypted message" is superfluous.

After considering the matter, applicant decided to eliminate the word "encrypted" and the term "without any encryption" and to return the language of the claims essentially to the language of the claims as originally filed. Applicant made this change after applicant noted that the Examiner did not reject the claims (as originally filed) under 35 U.S.C. 112, first paragraph. Applicant is confident, on the basis of the specification and the drawings, that a person of ordinary skill in the art would recognize that the word "message" by itself indicates that the "message" is unencrypted. This is particularly true since the specification discusses, and the claims recite, a digital signature of the message in addition to the message and the specification indicates quite clearly that the digital signature is an encrypted hash of the message.

By returning the claims essentially to their language in the application as originally filed and by eliminating the words "unencrypted" and "without any encryption" in the claims, applicant has eliminated any alleged problems raised by the Examiner under 35 U.S.C. 112, first paragraph and has accordingly reduced the issues in the application to a single issue that can be easily defined. The issue is whether the claims as now written in this amendment are allowable over the prior art cited by the Examiner. Applicant respectfully submits that all of the claims are allowable over the cited references (whether used individually or in combination) for a number of important reasons, all of which will be discussed in some detail below.

III. GLOBAL APPROACHES ESTABLISHING THE ALLOWABILITY OF APPLICANT'S CLAIMS OVER BARKAN

A. Either the word "message" (when used by itself) in the application indicates that the message is unencrypted or that it is encrypted. If the message is encrypted, the system described and claimed by applicant would be inoperative. The reason is that applicant has not indicated to the recipient in the application how to decrypt the encrypted message. Because of this, the word "message" in the claims has to be interpreted as meaning "unencrypted." In contrast, the Barkan reference cited by the Examiner in the Office Action dated March 18, 2005 discloses an encrypted message and a system for decrypting the message at a user 1 (the sender) and a user 2 (the recipient).

The Examiner has refused to allow applicant to designate the message as "unencrypted" in applicant's claims. For example, the Examiner has indicated the following on page 2 of the Office Action dated March 18, 2005:

> (1) "Claims 115-121, 145-150, 159-183, 187-191 and 226-242 are rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention."

The Examiner has further stated on page 4 of the Office Action:

> (2) "Claims 115,121, 145-150, 159-183, 187-191 and 226-242 are rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention."

The Examiner has based this rejection on the ground that it would require "undue experimentation to have the message be 'unencrypted.'"

The Examiner then has made the following statement on page 5 of the Office Action dated March 18, 2005:

> "While adding negative limitations like 'unencrypted' or 'without any encryption' or 'without encrypting' to the claim language, the instant application's specification clearly

shows digital signature as defined as encrypted message.
Thus, there is a contradiction."

There is no contradiction. Applicant always maintains the message in an unencrypted state even when applicant is obtaining the digital signature of the message. The reason is that the digital signature of the message is in addition to the message. It does not replace the message. Furthermore, the digital signature is encrypted (an encrypted hash of the message). Applicant has amended the claims to recite that the digital signature is in addition to the message. One purpose of this is to distinguish the digital signature of the message from the message. Another purpose is to indicate that the message remains unencrypted.

On the other hand, the Examiner has rejected applicant's claims as being unpatentable over Barkan by applying steps involving an "encrypted message" in Barkan against steps involving a "message" in applicant's claims. As applicant has previously indicated, a "message" in applicant's methods is not encrypted because there is no disclosure in applicant's specification that the recipient knows the code for decrypting ~~the~~an encrypted message. As a result, a considerable difference exists between a "message" as recited in the different steps in applicant's claims and an encrypted message as disclosed in the steps cited by the Examiner from the Barkan specification against applicant's claims.

B. As will be seen from the above discussion, the Examiner is unintentionally applying a double standard in rejecting applicant's claims. The Examiner is applying one standard -- a harsh standard -- in attempting to distinguish the words "unencrypted

message" in applicant's claims from the word "message" even though there is no difference between the meanings of the words "unencrypted message" and the word "message".

The Examiner is applying a different standard -- a lenient standard -- in interpreting the words "encrypted message" in Barkan to be equivalent to the word "message" in applicant's system. Applicant respectfully submits that the same standard should be applied to the word "message" in applicant's claims and to the words "encrypted message" in Barkan. By this consistent standard, the word "message" in applicant's claims should be interpreted as an "unencrypted message" and the words "encrypted message" in Barkan should be interpreted to include the word "encrypted". In applying this consistent interpretation, there is a considerable difference between the word "message" in applicant's claims and the words "encrypted message" in Barkan. This may be seen from the contorted steps that Barkan discloses for obtaining the decryption of the sender's (the user 1) message at the recipient (the user 2). This difference prevents Barkan from being a good prior art reference against applicant's claims.

C. All of applicant's claims recite a method including a number of steps performed at applicant's server. For example, applicant's server acts as a dispatcher and also acts as an authenticator. There is nothing in Barkan that is equivalent to applicant's server. The mail server 3 in Barkan does not operate as a dispatcher and also does not operate as an authenticator. The function of the mail server 3 in Barkan is to make the encryption of the user 1 known to the user 2 and the encryption of the user 2 known to

the user 1. Since applicant's system does not encrypt the message (except to provide a digital signature of the message in addition to the message) applicant does not provide a server with functions corresponding to the functions performed by the mail server 3 in Barkan. This causes applicant's system to operate completely differently from Barkan's system. For example, the mail server 3 in Barkan indicates to the user 1 how to encrypt a message from the user 2 so that it can be decrypted by the user 2 and the mail server 3 indicates to the user 1 how to encrypt a message from the user 2 so that it can be decrypted by the user 1. Applicant's system does not provide these functions. In applicant's system, the RPOST server receives a message from the sender and transmits the message to the destination address of the recipient. These differences in function between applicant and Barkan prevent Barkan from being a proper prior art reference against applicant's claims.

D. Barkan discloses nine (9) different methods. Each is significantly different from the others. It is accordingly not proper for the Examiner to reject a claim by citing individual method steps from different methods against the successive steps recited in any one of applicant's claims. For example, it is not proper for the Examiner to cite steps from method 3 in Barkan against a first step recited in a claim and steps from method 4 in Barkan against other steps recited in the claim. However, this is what the Examiner appears to have done time and time again to reject applicant's claims.

For example, the Examiner has applied different steps from individual methods in Barkan against the different steps recited in applicant's claim 115. This is shown on page 6 of the Office Action dated March 18, 2005. A table specifying the methods applied by

the Examiner against the successive steps recited in applicant's claim 115 is shown below:

Individual Steps Recited in Applicant's Claim 115:	Methods Cited in Barkan
Receiving message	2, 3
Transmitting the message	3, 4
Receiving at the server	2, 4
Providing at the server	4
Transmitting to the sender	4

As will be seen from the above chart, a single one of Barkan's nine (9) methods does not appear in all five (5) of the method steps recited in claim 115 when the portions cited by the Examiner from Barkan against each of the method steps are charted as shown above. Specifically, the Examiner applies method 4 against all of the steps recited in claim 115 but does not site method 4 against the first step in the claim. In effect, this constitutes an admission by the Examiner that claim 115 is allowable over Barkan.

E. One of the steps recited in claim 115 is that the RPOST server transmits the message to the destination address of the recipient. This constitutes a single step in claim 115. Barkan requires approximately six (6) steps to perform this relatively simple function. One reason is that the user 1's message is encrypted in Barkan when it is transmitted to the user 2. Because of this, for example, in Method 1 of Barkan, the user 1's message (a) is encrypted and (b) sent illustratively to the distribution center 63 in Figure 5 to obtain the public key of the user 2. Distribution center 63 then sends to the user 1 (c) a certificate identifying the public key of the user 2. The user 1 then (d) decrypts the certificate to obtain the public key of the user 2. The user 1 then (e) encrypts the message with the public key for the user 2 to create a second message. The user 1

then (f) sends the second message to the user 2. The user 2 then (g) decrypts the second message with the user 2's key to obtain the first (or original) message.

As will be seen, Barkan requires at least seven (7) steps to accomplish what applicant accomplishes in one (1) step. Applicant does not see how the Examiner can consider this complicated and convoluted approach in Barkan to correspond to applicant's single and simple step of transmitting the message (unencrypted) from the sender to the destination address of the recipient. This is particularly true since the user 1 in Barkan transmits the encrypted message (rather than the unencrypted message) to the user 2 and does this only after initially communicating with the distribution center 63. As will be appreciated, applicant's direct approach is also advantageous because there is a greater chance of committing an error in the seven (7) steps as in Barkan than in one (1) step as in applicant's system.

F. The flow of information in applicant's system is seamless. In other words, information flows from each station to the next without having to be returned to a previous station. For example, the message flows from the sender to the server, from the server to the destination address, from the destination address to the server and from the server to the sender. In effect, the information flows in a closed loop.

When the sender wishes to authenticate the message, the information flows from the sender to the RPOST server which authenticates, or denies the authentication of, the message. The server then indicates to the sender the results of the authentication operation.

The flow of information in Barkan is far from seamless. For example, in order for the sender (the user 1) in Barkan to transmit a message to the recipient (the user 2), the sender (the user 1) has to ask the server (the mail server 3) for the encryption code. The user 1 has to receive the user 2's encryption code from the mail server 3. The user 1 then has to encrypt the message with the encryption code of the user 2 and has to send the message with the encrypted code of the user 2 to the user 2. The user 2 then has to decrypt the message.

Thus, the RPOST server in applicant's system transmits the message (unencrypted) to the destination address in a single step. The use of at least seven (7) steps in Barkan is slower than the use of the single step by applicant. Furthermore, the chances of producing an error in Barkan's seven (7) steps are considerably greater than the chance of producing an error in applicant's single step.

The seamless flow of information in applicant's system may be seen from another standpoint. Because applicant's system is seamless, the RPOST server receives the message in each alternate step from a selected one of the sender and the destination address of the recipient and transmits the message to the other one of the sender and the destination address of the recipient. Furthermore, in the next two (2) steps of transmission, the RPOST server receives the message from the other one of the sender and the destination address of the recipient and transmits the message to the selected one of the sender and the destination address of the recipient. This is important because applicant's claims recite that all of the successive steps occur at the RPOST server.

Barkan does not operate in this way, particularly since the mail server 3 in Barkan does not receive the message in alternate steps and transmit the message in the other steps.

G. As will be seen, the destination address receives the message from the RPOST server whether or not the recipient at the destination address wishes to receive the message. This is an advantage from the sender's standpoint since the sender is the party that initiates the transmittal of the message. In Barkan, however, the recipient has to accept the message. If the recipient does not accept the message, the message from the sender is not delivered to the recipient. This is not desirable from the sender's standpoint since the sender desires the recipient to receive the message whether or not the recipient wishes to receive the message.

H. All of the claims being prosecuted in this application recite a series of steps that occur at the RPOST server and that involve the transmission or reception of data at the RPost server or the processing of data at the RPOST server. In each of these steps, the RPOST server either receives the message, processes the message or transmits the message. The mail server 3 in Barkan would probably be considered as corresponding to the RPOST server in applicant's system. However, the mail server 3 in Barkan does not operate the same way as the RPOST server. For example, the mail server 3 in Barkan does not either receive the message or transmit the message in each step. The mail server 3 in Barkan also does not process the message. The Examiner accordingly has had to cite steps that occur at the user 1 or the user 2 rather than at the mail server 3 to attempt to cite in Barkan what applicant recites in the claims. This prevents Barkan from constituting a good reference against applicant's claims.

IV. ANALYSIS OF EACH OF CLAIMS 115-121, 145-150 AND 230-243 ON A STEP-BY-STEP BASIS TO SHOW THE ALLOWABILITY OF EACH CLAIM OVER BARKAN

General Discussion

Claims 115-121, 145-150 and 230-242 have been rejected under 35 U.S.C. 102(b) as being anticipated by Barkan. As an example of this alleged anticipation, the Examiner has applied Barkan to claim 115 on an element-by-element basis. The Examiner has applied pages 9, 31 and 32 of Barkan against the recitation in claim 115 of the step of providing at the server the message from the sender. Barkan does not disclose on pages 9, 31 and 32 the step of receiving at the mail server 3 the message from the user 1. Furthermore, the message on these pages in Barkan is encrypted. Barkan also does not disclose the step of transmitting to the sender (the user 1) the message, and the digital signature of the message, for storage by the sender. The Examiner has cited page 33, first paragraph, to support his position. Page 33, first paragraph, of Barkan discloses that the "mail server 3 also sends the user 1 a message including the encrypted message from the user 2...." (Underlining supplied.) An encrypted message is not a digital signature of the message and is not even a digital fingerprint of the message. A digital signature of a message is an encrypted hash of the message and a digital fingerprint is a hash of the message. An encrypted message is not a hash of the message. So Barkan does not disclose a method of transmitting at the mail server 3 the message and the digital signature of the message.

As applicant's claims as now written, the claims recite a message. A message is not encrypted. This is particularly true since the Examiner has raised strong objections to the use by applicant of the terms "unencrypted message" and "without any encryption" in the claims. An "unencrypted message" has the same meaning as a "message" to a person of ordinary skill in the art. Since the use of the term "unencrypted message" is apparently strongly objectionable to the Examiner, the Examiner should have even stronger objections to the use of the term "message" to correspond to the use of the term "encrypted message." This is particularly true since a "message" and an "unencrypted message" are the same but a "message" and an "encrypted message" are quite different. Furthermore, applicant distinguishes in the specification and the claims between a message and an encrypted message by discussing a digital signature (an encrypted hash or an encrypted compression) in the specification and reciting a digital signature in the claims.

Claim 115

In citing different portions of Barkan against the successive steps in applicant's claim 115, the Examiner has cited portions in Barkan where Barkan is discussing an encrypted message. For example, the Examiner has cited steps a, b and c on page 12, step h on pages 23 and 24, and step d on page 30 of Barkan against the step recited by applicant in claim 115 of transmitting the message from the server to the destination address. In all of these portions in the Barkan specification, Barkan is discussing an encrypted message. The Examiner has cited the abstract in Barkan but the abstract is so

general and diffuse and so indefinite in language that it has no real meaning and cannot be properly cited against any of applicant's steps as recited in the claims.

The same discussion as in the previous paragraph applies to the step recited in applicant's claim 115 of receiving at the server an indication from a destination address that the message has been received at the destination address from the server. The Examiner has cited the abstract, page 8, page 19 and page 29 step c in Barkan against this step. As previously indicated, the abstract is so general, diffuse and indefinite that it has no meaning. The discussion on page 8 in Barkan is preliminary to the discussion of the nine (9) different methods in Barkan. Since the discussion on page 8 of Barkan is preliminary, it does not specifically disclose a step of receiving at the mail server 3 (the server) an indication from the user 2 (the destination address) that the message has been received at the user 2 from the mail server 3. Pages 19 and 29, step c also do not provide this disclosure. Furthermore, the message on page 19 and page 29 step c is encrypted. In addition, any message transmitted from the mail server 3 to the user 2 (the destination address) is encrypted so that it is not a "message" (unencrypted) such as recited by applicant in claim 115.

Claim 116

The Examiner has cited page 35, step 1 in Barkan against claim 116. In claim 116, the message and the digital signature of the message are recited as being discarded before any authentication occurs. On page 35, step 1 of Barkan, the message is discarded after authentication has occurred. There is a significant difference between discarding the message before authentication and discarding the message after authentication. It

may be logical to delete the message after the authentication of the message but it is not logical to delete the message before authenticating the message. Furthermore, the deletion of the message on page 35, step 1 of Barkan does not involve any deletion of the digital signature of the message in addition to the deletion of the message, as recited in claim 116. Claim 116 is also allowable over Barkan because of its dependency from allowable claim 115 and for the reasons specified in Section III.

As previously indicated, Barkan does not disclose the generation of a digital signature of the message after the delivery of the message to the destination address. This may be seen from the discussion above relating to claim 115. Page 34 step d in Barkan does not teach that the mail server 3 receives from the user 1 a copy of the message and the digital signature of the message before any authentication of the message but after the transmission of the message to the user 2. Furthermore, in pages 23-24 and 31-32 of Barkan, the user 2 encrypts the message as a step to indicate that he agrees to accept the message. Barkan additionally does not disclose on pages 22-24 and 31-32 that the mail server 3 generates digital fingerprints (hashes) of the message and the digital signature of the message and compares the fingerprints and authenticates the message on the basis of the comparison.

Claim 117

As previously indicated, Barkan does not maintain the message in its original state, and additionally generate a digital signature of the message, at the mail server 3. Since there is no generation of a digital signature of the message at the mail server 3 in Barkan, Barkan cannot transmit the message and the digital signature of the message

from the user 1 to the mail server 3. Furthermore, any transmission to the user 1 (the sender) in Barkan is in encrypted form. Because of this, the mail server 3 in Barkan does not generate digital fingerprints of the message, and of the digital signature of the message, such as recited in claim 117. Claim 117 is also allowable over Barkan because it is dependent from allowable claim 116 and for the reasons set forth in Section III.

Claim 118

The Examiner has cited pages 23, 29, 30 and 34 against the various steps recited in claim 118. Claim 118 recites various steps relating to an attachment and a digital signature of the attachment. Pages 23, 29, 30 and 34 in Barkan do not relate to an attachment such as recited by applicant in claim 118. Furthermore, pages 23, 29, 30 and 34 in Barkan do not relate to an attachment, and a digital signature of the attachment, such as recited by applicant in claim 118. Instead, pages 23, 29, 30, and 34 in Barkan relate to the processing of encryptions. As the Examiner will appreciate from his discussion on pages 2-5 of the Office Action relating to the alleged differences between a message and an unencrypted message and from the discussion in Section III, there is no difference between a message and an unencrypted message, but there is a considerable difference between a message and an encrypted message. Because of this, the Examiner cannot cite discussions in Barkan relating to the processing of an encrypted message to reject applicant's claims reciting steps relating to the processing of a message.

Pages 23, 29-30 and 34 do not disclose the following steps recited in claim 118 when applied to the Barkan patent:

(a) providing at the mail server 3 an attachment, including the identity of the user 1 and the address of the mail server 3 and the destination address of the user 2;

(b) maintaining at the mail server 3 the attachment and additionally providing the digital signature of the attachment; and

(c) transmitting from the mail server 3 to the user 1 the attachment including the identity of the user 1, the identity and address of the mail server 3 and the identity and the address of the user 2 and transmitting from the mail server 3 to the user 1 the attachment, and the digital signature of the attachment, at the same time as the transmission of the message, and the digital signature of the message, to the user 1.

Claim 118 is also allowable over Barkan because of its dependency from claim 116 and for the reasons set forth in Section III.

Claim 119

The Examiner has cited the following portions of Barkan to reject claim 119: (a) the abstract, Pages 8, 19 and 29 (step c) against the recited step of receiving an attachment from the destination address and (b) pages 23, 29-30 and 34 against the recited steps of maintaining at the server the attachment in the original form of the attachment, and additionally providing the digital signature of the attachment in the original form of the attachment, and transmitting to the sender the attachment and the digital signature of the attachment. Barkan does not disclose an attachment on pages 23, 29-30 and 34 or on pages 8, 19 and 29 step c and does not disclose on these pages the

additional provision of a digital signature of the attachment and the transmittal of the attachment and the digital signature of the attachment from the mail server 3 to the user 1. Furthermore, documentary material disclosed in Barkan as being transmitted on these pages is described as being encrypted. As applicant has previously indicated, any disclosure in Barkan of the processing of an encrypted message is not equivalent to the recitation by applicant in the claims of the processing of a message.

Barkan also does not receive an attachment at the mail server 3 (the server) from the user 2 in claim 119. Barkan also does not maintain the attachment at the mail server 3 and additionally provide at the mail server 3 the digital signature of the attachment. Barkan further does not transmit from the mail server 3 (the server) to the user 1 (the sender) the attachment and the digital signature of the attachment. Claim 119 is also allowable over Barkan because it is dependent from allowable claim 115 and for the reasons set forth in Section III.

Claim 120

Claim 120 recites that the RPOST server receives from the sender the message, the digital signature of the message, the attachment and the digital signature of the attachment. There is nothing in Barkan corresponding to the RPOST server. Certainly, the mail server 3 does not correspond to the RPOST server. Furthermore, nothing in Barkan (including the mail server 3) corresponds to the RPOST server in receiving the message, the digital signature of the message, the attachment and the digital signature of the attachment from the sender (the user 1) in Barkan. Since nothing in Barkan (including the mail server 3) receives the message, the attachment and the digital

signatures of the message and the attachment, nothing in Barkan (including the mail server 3) generates digital fingerprints of the message, the attachment and the digital signatures of the message and the attachment. In addition, anything disclosed on pages 23-24 steps j-h, 29-30, 31-32 and 34 in Barkan is encrypted. This is contrary to applicant's system since the message and the attachment in applicant's system remain unencrypted even though digital signatures are additionally provided of the message and the attachment.

Claim 121

In claim 121, applicant recites the steps of receiving the message and the digital signature of the message at the server from the sender and authenticating the message at the server on the basis of the message and the digital signature of the message received by the server from the sender. The mail server 3 in Barkan does not perform these functions. Neither does the user 2 and the mail box of the user 2. Furthermore, pages 23-24 steps j-h and pages 29-30 in Barkan do not disclose these functions. For example, the mail server 3 in Barkan does not receive the message and the digital signature of the message from the user 1. Furthermore, the user 2 (not the mail server 3) in Barkan authenticates the message that it receives from the user 1. This is quite different from the authentication of the message by the RPOST server in applicant's system. Furthermore, the message is encrypted in Barkan, but is not encrypted in applicant's system. Claim 121 is also allowable over Barkan because of its dependency from allowable claim 119 and for the reasons set forth in Section III.

Claim 145

Barkan's analysis of claim 145 has substantially the same deficiencies as set forth above. For example, the RPOST server in applicant's system receives the message from the sender, transmits the message to the destination address of the recipient and thereafter authenticates the message. The mail server 3 in Barkan does not receive the message from the user 1, transmit the message (unencrypted) to the user 2 and thereafter authenticate the message. This results partly from the fact that the message transmitted from the mail server 3 in Barkan to the user 2 is encrypted and partly from the fact that the mail server 3 does not authenticate the message from the user 1. Rather, the user 2 in Barkan authenticates the message from the user 1. Furthermore, the mail server 3 in Barkan does not transmit the message through a path including servers between the mail server 3 and the destination address (the user 2). The mail server 3 in Barkan further does not transmit to the user 1 the message and the path of transmission of the message between the mail server 3 and the destination address (the user 2). In view of the above, the abstract and page 9, 13, 19 step b, 22, 23-24 step h, and 31-32 do not disclose any of the steps recited in claim 145. Claim 145 is also allowable over Barkan for the reasons discussed in Section III.

Claim 146

In applicant's system, the RPOST server receives from the sender the message and the path of transmission of the message between the server and the destination address. This is recited in claim 146. Contrary to the position of the Examiner, the mail server 3 in Barkan does not receive the message or the path of transmission of the message

between the mail server 3 and the user 2. Furthermore, the mail server 3 in Barkan does not authenticate the message. This may be seen from the statement by Barkan in section 2 at the bottom of page 31 and the top of page 32 where Barkan indicates that the user 2 authenticates the message. Furthermore, the user 2 in Barkan authenticates the message by operating upon an encrypted message. As previously explained, these are fundamental differences between applicant's system and Barkan.

There is another important difference between applicant's system as recited in claim 146 and Barkan. The user 2 in Barkan does not authenticate the message on the basis of the path of transmission of the message between the mail server 3 and the user 2. The user 2 authenticates the message on the basis that the message is encrypted in accordance with the user 2's encryption key and that the user 2 is able to decrypt this encryption by using the user 2's decryption key. Since claim 146 is dependent from allowable claim 145, claim 146 is also allowable over Barkan for the same reasons as claim 145. Claim 146 is also allowable over Barkan for the reasons set forth in Section III.

Claim 147

There is another fundamental difference between applicant's system and Barkan and this is recited in claim 147. Applicant does not retain the message and the path of transmission of the message. This occurs after the RPOST server transmits the message and the path of transmission of the message to the sender but before the RPOST server authenticates the message. Barkan does not retain the message after he authenticates the message. Barkan discloses this on page 35, step 1. Barkan's system would not be

operative if he deleted the message before authentication occurred. Furthermore, the user 2 in Barkan does not authenticate the message on the basis of the path of transmission of the message between the mail server 3 and the user 2. Barkan authenticates the message at the user 2 on the basis that the message is encrypted with the encryption key of the user 2.

Claim 148

Claim 148 is allowable over Barkan because it is dependent from allowable claim 145.

Claim 149

With respect to claim 149, the user 2 (the destination address) in Barkan does not authenticate the message on the basis of the path of transmission of the message between the server (the mail server 3) and the destination address (the user 2). The user 2 in Barkan authenticates the message on the basis of the encryption of the message. Perhaps because of this, Barkan does not indicate whether the path of transmission of the message between the mail server 3 and the user 2 includes the identity and address of the user 1 and the identity of the user 2. This is recited in claim 149. Since Barkan does not disclose this on pages 23, 29-30 and 34 and since Barkan authenticates the message on the basis of the encryption of the message, claim 149 is allowable over Barkan. Claim 149 is also allowable over Barkan because of its dependency from allowable claim 145 and for the reasons set forth in Section III.

Claim 150

In claim 150, applicant recites that the RPOST server does not retain the message and the path of the transmission of the message between the server and the destination address after it transmits to the sender the message and the path of transmission of the message between the server and the destination address but before any authentication of the message. The Examiner has cited pages 23, 29-30, 34 and 35 step 1 against the recitation in claim 150. As previously indicated above in connection with claim 146, the message is not deleted in Barkan until after the authentication has occurred. When the message has been authenticated, it is not important to retain the message. Furthermore, the mail server 3 in Barkan does not delete the message. The user 2 in Barkan deletes the message. Barkan also does not have an attachment. Furthermore, claim 150 is dependent from allowable claim 146 and is accordingly allowable over Barkan for the same reasons as claim 146. Claim 150 is also allowable over Barkan for the reasons set forth in Section III.

Claim 230

Claim 230 is allowable for certain important reasons over Barkan's (a) abstract, (b) page 12, steps a, b and c, (c) pages 23-24, step h, (d) page 30, step d, (e) page 33, first paragraph and (f) page 34. None of the cited portions of Barkan discloses, in a method, the steps of providing an attachment including the identity and address of the user 1, the identity and address of a second server (the RPOST server in applicant's system and the mail server 3 in Barkan) and the identity and destination address of the user 2. The cited

portions of Barkan also do not disclose the step of transmitting the electronic attachment from the second server (the mail server 3) to the sender (the user 1).

The abstract in Barkan is so general, diffuse and indefinite that it has no real significance when applied to specific steps such as recited in claim 230. Steps a, b and c on page 12 of Barkan deal with a message and not an attachment. Furthermore, the message in Barkan is encrypted. As previously indicated, there is a considerable difference between a message in applicant's system and an encryption of the message as in Barkan. Furthermore, the message on page 12, steps a, b and c in Barkan is transmitted to the user 2 (the recipient) rather than to the user 1 (the sender) in Barkan. In addition, the document on page 12 in Barkan is a message rather than an attachment. And the event does not occur in Barkan in a member (the mail server 3) corresponding to the RPOST server.

The discussion on pages 23-24 step h in Barkan presents the same problems as discussed above with respect to page 12, steps a, b and c in Barkan. The document on pages 23-24, step h and on page 30, step d is a message and not an attachment. Furthermore, it is encrypted rather than being unencrypted. It is transmitted to the user 2 (the recipient) rather than to the user 1 (the sender) and the intermediary 71 does not correspond to the RPOST server. Thus, the event specified in claim 230 does not occur at a server (the mail server 3) corresponding to the RPOST server.

The Examiner has also cited page 33, first paragraph, in Barkan as prior art against claim 230. The document being sent in Barkan is a message rather than an attachment and it is encrypted. Furthermore, it is not the message provided by the user 1 (the sender)

since it is from the user 2 (the recipient). And it does not occur at a server (the mail server 3) corresponding to the RPOST server. The document is also not sent to the user 1 (the sender) by a server (the mail server 3) corresponding to the RPOST server. The document sent to the user 2 (the recipient) in Barkan also does not include the identity and address of the sender (the user 1) and the identity and address of the mail server 3 (allegedly corresponding to the RPOST server) and the identity and address of the user 2 (the destination server).

There is also a citation by the Examiner of page 34 in Barkan against claim 230. Page 34 presents the same difficulties to the Examiner as the other portions of Barkan cited by the Examiner against claim 230. The document in Barkan is a message rather than an attachment and it is encrypted rather than being unencrypted. Whether the document is a message or an attachment, it does not include the identity and address of the sender (the user 1) and the identity and address of a server (the mail server 3) corresponding to the RPOST server and the identity and address of the user 2 (the recipient). Furthermore, the document on page 34 of Barkan is not transmitted from the mail server 3 (allegedly corresponding to the RPOST server) to the user 1 (the sender).

To summarize the discussion above with respect to claim 230, Barkan does not provide at the mail server 3 an attachment including the identity and identity of the user 1 and the identity and address of the mail server 3 and the identity and address of the user 2. Barkan also does not transmit the attachment from the mail server 3 to the user 1. Claim 230 is also allowable over Barkan for the reasons set forth in Section III.

Claim 231

The Examiner has cited page 44, step e of Barkan against claim 231, which recites that the electronic attachment includes the address and identity of intermediate servers receiving the electronic message in the transmission of the electronic message between the second server and the destination server. Applicant respectfully submits that page 44, step e in Barkan does not provide a disclosure of applicant's recitation in claim 231. Claim 231 is also allowable over Barkan for the same reasons as claim 230 because it is dependent from claim 230. Claim 231 is additionally allowable over Barkan for the reasons set forth in Section III.

Claim 232

The abstract, page 12 steps a, b and c, pages 23-24 step h, page 30 step d, page 33 first paragraph and page 34 in Barkan have been cited by the Examiner against claim 232. However, Barkan does not disclose the step of maintaining the electronic attachment in its original form, and additionally providing a digital signature of the electronic attachment, at the second server (the mail server 3). Since Barkan does not disclose the generation of the digital signature (the encrypted hash) from the second server (the mail server 3), Barkan does not disclose the step of transmitting the digital signature of the attachment from the second server (the mail server 3) to the sender (the user 1) at the time of transmitting the electronic attachment from the mail server 3 to the user 1. Claim 232 is also allowable over Barkan for the same reasons as claim 230 because of its dependency from allowable claim 230. Claim 232 is also allowable over Barkan for the reasons set forth in Section III.

Specifically, Barkan does not teach on page 44 steps that the electronic attachment includes the address and identity of intermediate stations receiving the electronic attachment in the transmission of the electronic attachment between the mail server 3 and the user 2. One reason is that Barkan does not disclose intermediate stations such as recited in claim 232. Another reason is that the message in Barkan is encrypted.

Claim 233

Since claim 233 is dependent from allowable claim 231, it is allowable over Barkan for the same reasons as claim 231. Claim 233 is also allowable over Barkan for the reasons set forth in the previous paragraph. Claim 233 is additionally allowable over Barkan for the reasons set forth in Section III.

Claim 234

In claim 234, there is a recitation of the step of receiving the electronic attachment, and the digital signature of the electronic attachment, at the second server from the sender. A recitation is also made in claim 234 of the step of authenticating the electronic attachment at the second server on the basis of the electronic attachment, and the digital signature of the electronic attachment, received by the second server from the sender. The portions of Barkan cited by the Examiner against claim 234 do not disclose the steps of receiving the attachment and the digital signature of the attachment at the mail server 3 from the user 1 and authenticating the attachment at the mail server 3 on the basis of the attachment, and the digital signature of the attachment, received by the mail server 3 from the user 1. Claim 234 is also allowable over Barkan because of its dependency from allowable claim 231 and for the reasons set forth in Section III.

Claim 235

Pages 23-24 steps j-h and pages 31-32 in Barkan have been cited by the Examiner against claim 235. Claim 235 recites the step of authenticating the electronic attachment at the second server on the basis of the electronic attachment, and the digital signature of the electronic attachment, received by the second server from the sender. Pages 23-24, steps j-h and pages 31-32 cited by the Examiner in Barkan do not disclose an electronic attachment or a digital signature of the electronic attachment. Because of this, these pages cannot disclose the step of authenticating the electronic attachment at the second server (the mail server 3) on the basis of the electronic attachment, and the digital signature of the electronic attachment, received by the second server from the sender (the user 1). Claim 235 is also allowable over Barkan because it is dependent from allowable claim 233 and for the reasons set forth in Section III.

Claim 236

Claim 236 recites the additional steps of receiving the attachment, and the digital signature of the attachment, at the second server from the sender, providing at the second server digital fingerprints of the electronic attachment, and the digital signature of the electronic attachment, received at the second server from the sender and comparing the digital fingerprints to authenticate the electronic attachment. The portions of Barkan cited by the Examiner against claim 236 do not disclose these features. In other words, Barkan does not provide digital fingerprints (hashes) of the attachment and the digital signature of the attachment. Since Barkan does not provide the digital signature, Barkan cannot compare the digital fingerprints to authenticate the attachment at the mail server 3.

Since claim 236 is dependent from claim 232, claim 236 is also allowable over Barkan for the same reasons as claim 232. Claim 236 is additionally allowable over Barkan for the reasons set forth in Section III.

Claim 237

Claim 237 is dependent from claim 232 and is accordingly allowable over Barkan for the same reasons as claim 232. Claim 237 is also allowable over Barkan for the reasons discussed in the previous paragraph.

Claim 238

Claim 238 is also allowable over Barkan for certain important reasons. This may be seen from the following:

a. The abstract, pages 23-24 step (h) and page 19 step b in Barkan do not disclose the step of transmitting an electronic message between the server (the mail server 3) and the destination address (the user 2). Furthermore, transmitting an encrypted message between the server (the mail server 3) and the destination address (the user 2) is not the same as, and does not even correspond to, transmitting a message (unencrypted) between the server and the destination address. Furthermore, the mail server 3 in Barkan is not the same as, and does not correspond to, the RPOST server in the claims.

b. Pages 13 and 22-24 in Barkan do not disclose the step recited in claim 238 of receiving at the server (the mail server 3) the path of transmission of the electronic message between the server and the destination address (the user 2), the path including servers between the server (the mail server 3) and the

destination address (the user 2). Barkan makes the following statement on page 13:

"Link 11 may be implemented with any combination of a wide variety of communication means as known in the art, like telephone lines, wireless, local area network (LAN) and/or Internet links."

Link 11 is between the user 1 and the mail box 12 of the user 1 in Barkan. The likelihood of servers in the link 11 would accordingly be quite small. Link 11 is not between the user 1 and the user 2 or between either of the users and the mail server 3. Furthermore, Barkan does not disclose that there are, or even may be, servers between the user 1 and the user 2, or between either one of the user 1 or the user 2 and the mail server 3.

Barkan also does not disclose on pages 13 and 22-24 that the mail server 3 in Barkan receives the path of transmission of the electronic message (as distinguished from the encrypted electronic message) between the server (the mail server 3) and the destination address (the user 2). Barkan further does not disclose that the path includes servers between the server (the mail server 3) and the destination address (the user 2).

c. Pages 9, 13, 22-24 and 31-32 in Barkan do not disclose a path of transmission of the message between the server (the mail server 3) and the destination address (the user 2).

d. Claim 238 is also allowable over Barkan for the global reasons set forth in Section III.

In claim 238, the server is recited. In this application, the server is the RPOST server. As applicant has indicated previously, there is nothing in Barkan that is the same as (or that corresponds to) the RPOST server. The mail server 3 in Barkan certainly does not transmit the message to the user 1 and the user 2. Instead, the mail server 3 in Barkan provides the user 2's encryption key to the user 1 so that the user 1 can encrypt the message with the user 2's encryption key. The user 2 can then decrypt the message when the user 2 receives the encrypted message from the user 1.

Claim 239

The Examiner has cited page 35 step 1 in Barkan against claim 239. However, as applicant has previously indicated, page 35 step 1 in Barkan specifies that the message is deleted after authentication has been provided. In contrast, applicant deletes the message before authentication has been provided. It may be logical to delete the message after authentication is provided. It is not logical to delete the message before authentication is provided. Claim 239 is also allowable over Barkan for the global reasons set forth in Section III. Claim 239 is additionally allowable over Barkan because it is dependent from allowable claim 238.

Claim 240

In claim 240, applicant recites the step that the server receives from the sender the message and the path of transmission of the message between the server and the destination address. Applicant has previously indicated in claims 237 and 239 why Barkan does not disclose this step. Furthermore, the mail server 3 in Barkan does not

receive from the user 1 the message and the path of transmission of the message between the mail server 3 and the user 2.

There is also a recitation in claim 240 that the server authenticates the message on the basis of the message, and the path of transmission of the message between the server and the destination address, received by the server from the sender. The Examiner has cited pages 23-24 steps j-h and pages 31-32 in Barkan against the recitation of this step. Applicant has previously indicated in claims 238 and 239 why these pages do not support the recitation of this step. Furthermore, the mail server 3 in Barkan does not authenticate the message. Claim 240 is also allowable over Barkan for the global reasons set forth in Section III. Claim 240 is additionally allowable over Barkan because of its dependency from allowable claim 238.

Claim 241

Claim 241 recites that the server provides a digital signature of the electronic message and additionally provides a digital signature of the electronic message. There is also a recitation in claim 241 that the server receives from the sender the electronic message and the digital signature of the electronic message. A further recitation is made in claim 241 that the server provides digital fingerprints of the electronic message and the digital signature of the electronic message and compares the digital fingerprints to authenticate the electronic message. The Examiner has cited the abstract, page 12 steps a, b and c, pages 23-24 steps j-h and pages 31-32 in Barkan against claim 241. Claim 241 is allowable over Barkan for the reasons discussed in claims 115 and 117. Claim 241

is also allowable over Barkan because it is dependent from allowable claim 240. Claim 241 is additionally allowable over Barkan for the global reasons set forth in Section III.

Claim 242

The Examiner has cited the abstract, page 12 steps a, b and c, pages 23-24 steps j-h and pages 31-32 in Barkan against claim 242 and has rejected claim 242 on the basis of these citations. Claim 242 is allowable over Barkan for the same reasons as claim 239 because it is dependent from claim 239. Claim 242 is also allowable over Barkan because the cited portions of Barkan do not disclose that the server (the mail server 3) maintains the path of transmission of the message in its original form and additionally provides a digital signature of the path of transmission of the electronic message between the server (the mail server 3) and the destination address (the user 2). Barkan does not provide a path of transmission and the digital signature of the path of transmission and does not provide a server (the mail server 3) that is the same as, or that corresponds to, the RPOST server to provide the path of transmission and the digital signature of the path of transmission. Barkan also does not provide for the mail server 3 to receive from the user 1 the path of transmission and the digital signature of the path of transmission. Barkan additionally does not disclose that the mail server 3 provides digital fingerprints of the path of transmission and the digital signature of the path of transmission and compares the digital fingerprints to authenticate the message. Claim 242 is also allowable over Barkan for the global reasons set forth in Section III.

V. ANALYSIS ON A GLOBAL BASIS OF THE PATENTABILITY OF CLAIMS

OVER THE COMBINATION OF BARKAN AND ZABETIAN

A. A number of the claims have been rejected as unpatentable over a combination of Barkan and Zabetian. These claims are allowable on a global basis over Barkan for the reasons set forth in Section III. The claims are also allowable over Zabetian for the same reasons. Since both Barkan and Zabetian fail to disclose the same features recited in the claims, the claims are allowable over the combination of Barkan and Zabetian.

B. Applicant is not contending that he is the first to provide SMTP and ESMTP protocols. Applicant does believe, however, that he is the first to use the SMTP and ESMTP protocols to provide an authentication of a message and to verify a number of parameters related to the message authentication, including the server, the destination address, the time of the transmittal of the message from the server to the destination address, the time of reception of the message at the destination address, and the opening of the message at the destination address. Furthermore, applicant respectfully submits that the use by applicant of the SMTP and ESMTP protocols to provide the authentication and the verification specified in the previous sentence would not have been obvious to a person of ordinary skill in the art. This will be substantiated from a discussion of the law subsequently in this amendment.

C. Zabetian filed his application in the USPTO on July 2, 1997. Zabetian indicates in column 4, line 31, that the use of the SMTP code is "conventional." This would indicate that the SMTP code was "conventional" for a number of years prior to 1997. In all of these years until the filing of this application in the USPTO in July, 2000,

the use of the SMTP code in an authenticating system to provide for an authentication or verification of a message was apparently not known. In an art advancing as rapidly as the computer art during that period, the failure of recognizing the use, and the advantage of use, of the SMTP protocol or the ESMTP protocol to provide the authentication of a message and the verification of related parameters was the equivalent of a lifetime in other less advanced arts. This would indicate that it would not have been obvious to a person of ordinary skill in the art to use the SMTP and the ESMTP protocols in authenticating a message and verifying parameters related to the message authentication..

D. The Examiner has made the following statement on page 36 of the Office Action dated 03/18/2005:

> "In response to applicant's arguments against the references individually, one cannot show non-obviousness by attacking references individually where the rejections are based on combinations of references. (Citing legal references.) Applicant obviously attacks references individually without taking into consideration based on the teaching of combinations of references as shown above."

The Examiner has misinterpreted applicant's statements in the amendment filed by applicant on October 25, 2004. For example, applicant stated as follows on page 123 of the amendment dated October 25, 2004:

> "All of claims 115-121, 145-150, 159-183, 187-191 and 220-260 are allowable over Barkan, and the combination of Barkan and Zabetian, for the reasons set forth in subsections (B)(1) (a-e)."

Subsequently, on page 123 of the amendment, applicant stated:

> "However, since neither Zabetian nor Barkan teaches what is discussed in subsections (B)(1)(a) – (B)(1)(e), all of the claims are allowable over the combination of Barkan and Zabetian for the reasons set forth in subsections (B)(1)(a) – (B)(1)(e).
>
> "Starting with subsection (B)(1)(f) and extending through subsection (B)(1)(a-b), individual ones of the claims are allowable over Barkan, and the combination of Barkan and Zabetian, because the individual ones of the claims recite what is specified in that subsection and because the references do not disclose what is specified in the subsection." (Underlining supplied.)

Applicant respectfully submits that the quotations above from the amendment dated October 25, 2004 make it quite clear that applicant is indicating that each of applicant's claims is allowable over the combination of Barkan and Zabetian because each of the references fails to disclose the same method steps recited in the claim. Therefore, the combination of Barkan and Zabetian also fails to disclose these same features.

E. On page 15 and 16 of the Office Action dated 03/19/2005, the Examiner states:

> "However, Barkan does not explicitly teach transmitting a message via a protocol selected from a group consisting of an SMTP protocol and an ESMTP protocol. Zabetian teaches the electronic documents send (sic) between clients and servers using conventional protocols such as SMTP,

FTP, HTTP, and other network protocol could be used to transmit electronic documents (col. 4 lines 25-55, col. 6 lines 21-37, col. 14 lines 53-66). It would have been obvious to one of ordinary skill in the Data Processing art at the time of the invention was made to combine the teachings of Barkan and Zabetian to include the step of using a protocol selected from a group of network conventional protocols because it would have an efficient communications system that has a capability for users to send and attach various kinds of files to electronic mail (including electronic document certification, verification, digital signature)."

Applicant is not claiming that he is the first to send electronic mail via an SMTP or an ESMTP protocol. Applicant does believe, however, that he is the first to use an SMTP or ESMTP protocol to authenticate a message and to provide verification of various parameters relating to the authentication. Zabetian may mention certification in his patent but he does not indicate anywhere in the patent that the SMTP or ESMTP protocol is used to provide the authentication or certification. Because of this, Zabetian cannot be used as a prior art reference to establish that it would have been obvious to a person of ordinary skill in the art to use the SMTP or ESMTP protocol for authenticating the message and verifying various parameters relating to the message.

F. The Examiner has cited various court decisions on pages 36 and 37 of the Office Action dated 04/14/05. All of these court decisions (except for In re Merck & Co. on page 36) are decisions from the CCPA with dates in the year 1981 or in years preceding 1981 and going back to 1969. All of these decision precede the Federal Circuit

Court of Appeals. These decisions have been superceded by decisions of the Federal Circuit Court of Appeals. For example, the Federal Circuit Court of Appeals held in 1984 that, in order for different prior art references to be combined to reject a claim, the references have to disclose or suggest the combination recited in the claim. ACS Hospitality Systems, Inc. v. Montefiore Hospital, 732 F.2d 1572, 221 USPQ 929 (Fed. Cir. 1984). As the Federal Circuit indicated in the ACS case at 732 F.2d 1572, 1577, 221 USPQ 929, 933:

> "Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention absent some teaching or suggestion supporting the combination. Under Section 103, teaching of references can be combined only if there is some suggestion or incentive to do so."

See also In re Fine, 837 F.2d 1071, 5 USPQ 2d 1596 (Fed. Cir. 1988) and In re Jones, 958 F.2d 347, 21 USPQ 2d 1941 (Fed. Cir. 1992) in support of the holding in the ACS case.

Neither Barkan nor Zabetian cited by the Examiner to reject the claims in this application discloses or suggests certain of the features recited in the claims, the features being the same for Barkan and Zabetian. These features will be discussed on a claim-by-claim basis. The references cannot accordingly be combined to reject the claims.

VI. ALLOWABILITY OF CLAIMS 159-183, 187-191 AND 226-229 OVER THE COMBINATION OF BARKAN AND ZABETIAN

General Discussion

Claims 159-182, 187-191 and 226-229 have been rejected under 36 U.S.C. 103(a) as being unpatentable over Barkan in view of Zabetian. Claims 159-183, 187-191 and 226-229 are allowable for certain important reasons over the combination of Barkan and Zabetian.

Claim 159

Claim 159 is allowable over the combination of Barkan and Zabetian for the reasons discussed in Sections III and V. Claim 159 is also allowable over Barkan because Barkan does not disclose the step of receiving at the server (the mail server 3) the electronic message from a sender (the user 1) for transmission by the server to the destination address (the user 2). Barkan does not disclose in the abstract, pages 23-24 and page 19 step b the step of receiving at the mail server 3 an electronic message from the user 1 for transmission to the user 2. Furthermore (a) the abstract, (b) page 12 steps a, b and c, (c) pages 23-24 step h and (d) page 30 step d in Barkan do not disclose the step of transmitting the message (as distinguished from an encrypted message in Barkan) from the mail server 3 to the user 2. There is also no disclosure in Barkan (abstract and pages 8, 19 and 29 step c) of the step of receiving at the mail server 3 the transmission of the electronic message between the mail server 3 and the user 2. In the cited portions of Barkan, the mail server 3 does not receive the transmission of the electronic message between the mail server 3 and the user 2.

It should be noted that claim 159 recites that all of the recited steps are performed at the server (the RPOST server). The mail server 3 in Barkan does not perform any of

the steps recited in claim 159 and certainly does not disclose that all of these steps are performed at the mail server 3. The claims are allowable over Zabetian for the same reasons as they are allowable over Barkan. Furthermore, neither Barkan nor Zabetian uses an SMTP or an ESMTP protocol to authenticate a message or verify parameters relating to the message. Claim 159 is also allowable over the combination of Barkan and Zabetian for the reasons specified in Sections III and V.

Claim 160

Claim 160 is allowable over the combination of Barkan and Zabetian for the same reasons as claim 159 because it is dependent from claim 159. Claim 160 is also allowable over the combination of Barkan and Zabetian because of the positions set forth in Sections III and V of this amendment. Furthermore, any transmission between the mail server 3 and the user 2 on pages 23, 29-30 and 34 in Barkan does not include the identity of the user 1 and the identity and address of the mail server 3 and the user 2, this relationship being absent from the disclosure on pages 23, 29-30 and 34 of Barkan. In addition, since the transmission between the mail server 3 and the user 2 in claim 160 is recited as being the transmission of the message, Barkan does not meet the conditions of claim 160 since Barkan transmits the encrypted message and not an unencrypted message. Claim 160 is also allowable over the combination of Barkan and Zabetian for the reasons specified in Sections III and V.

Claim 161

Since claim 161 is dependent from claim 159, it is allowable over the combination of Barkan and Zabetian for the same reasons as claim 159. Claim 161 is also allowable

over the combination of Barkan and Zabetian for the reasons set forth in Sections III and V. Claim 161 is additionally allowable over the combination of Barkan and Zabetian because it recites the steps of providing a transmission of the message from the server to the sender and including, in the transmissions from the server to the sender, the electronic message and additionally a digital signature of the electronic message. Barkan does not send his message from the mail server 3 to the user 1. Even if Barkan should provide such a transmission, Barkan also does not include, in such transmission, the electronic message and additionally a digital signature of the user 1's message.

Because of its dependency from claim 159, claim 162 is allowable over the combination of Barkan and Zabetian for the same reasons as claim 159. Actually, the mail server 3 in Barkan does not transport the message to the user 2. Because of this, the mail server 3 in Barkan does not record the time for the transmission of the electronic message from the mail server 3 to the user 2 and the time for the receipt of the electronic message at the user 2. Claim 162 is also allowable over Zabetian for the same reasons as it is allowable over Barkan. Claim 162 is also allowable over each of Barkan and Zabetian because neither reference discloses the use of the SMTP and ESMTP protocols to authenticate the message and verify certain parameters (e.g., time for the transmission and reception of the message) related to the message. Claim 162 is also allowable over the combination of Barkan and Zabetian for the reasons specified in Sections III and V.

Claim 163

Claim 163 is allowable over the combination of Barkan and Zabetian for the reasons specified above with respect to claims 161 and 162. Claim 163 is also allowable

over the combination of Barkan and Zabetian because it is dependent from allowable claim 160 and for the reasons specified in Sections III and V.

Claim 164

Claim 164 is allowable over the combination of Barkan and Zabetian because it is dependent from allowable claim 159. Claim 164 additionally recites the step of including, in the transmission of the electronic message between the server and the destination address, the status of the delivery of the electronic message at the destination address from the server 2. The Examiner has cited the abstract and pages 8, 9, 19, 22-24, 28-29 step c, 31-32 and 51 in Barkan. These pages in Barkan does not disclose the status of the delivery of the electronic message at the user 2 from the mail server 3. Claim 164 is allowable over Zabetian for the same reasons that it is allowable over Barkan. Furthermore, neither Barkan nor Zabetian discloses the use of the SMTP and ESMTP protocols to verify the status of delivery of the message at the user 2 from the mail server 3. Claim 164 is also allowable over the combination of Barkan and Zabetian for the reasons specified in Sections III and V.

Claim 165

The Examiner has cited the abstract and pages 8, 19, 29 step c, 31, 35 and 51 in Barkan against the recitations in claim 165. However, Barkan does not disclose the step of receiving at the mail server 3 a delivery status notification relating to the status of the delivery of the electronic message to the user 2. Claim 165 is also allowable over Zabetian for the same reasons that it is allowable over Barkan. Claim 165 is dependent from claim 159 and is accordingly allowable over the combination of Barkan and

Zabetian for the same reasons as claim 159. Claim 165 is also allowable over the combination of Barkan and Zabetian for the reasons specified in Sections III and V.

Claim 166

Barkan does not disclose the following steps recited for the first server (the RPOST server) in claim 166:

1. Receiving, at the mail server 3 from the user 2 the transmission between the mail server 3 and the user 2 of the electronic message, and

2. Transmitting from the mail server 3 to the user 1 the electronic message and the transmission between the mail server 3 and the user 2 in the selected one of the SMTP and ESMTP protocols.

The mail server 3 in Barkan does not disclose these functions, particularly since the mail server 3 operates to provide encryptions. There is also no server in Zabetian that performs the functions specified above. Claim 166 is additionally allowable over Zabetian because Zabetian does not use the SMTP and ESMTP protocols to authenticate the message and verify parameters related to the message. Claim 166 is also allowable over the combination of Barkan and Zabetian for the reasons specified in Sections III and V.

Claim 167

Because of its dependency from claim 166, claim 167 is allowable over the combination of Barkan and Zabetian for the same reasons as claim 166. Claim 167 is also allowable over the combination of references for the reasons set forth in Sections III and V. Furthermore, the mail server 3 in Barkan does not perform the step of

transmitting from the mail server 3 to the user 1 the electronic message at the time of the completion of the transmission of the electronic message between the mail server 3 and the user 2. In addition, Zabetian does not use the SMTP and ESMTP protocols to authenticate the message and to verify parameters relating to the message. There is also no server in Zabetian that performs this function.

Claim 168

In the RPOST system, the RPOST server discards the electronic message at the RPOST server after the transmission of the electronic message by the RPOST server to the sender but before the authentication of the message. This is recited in claim 168. Barkan discards the message but it is after the authentication. Zabetian does not dispose of the message. Because of this, claim 168 is allowable over the combination of Barkan and Zabetian. Claim 168 is also allowable over the combination of Barkan and Zabetian because of its dependency from allowable claim 166 and for the reasons set forth in sections III and V. Claim 168 is also allowable over Zabetian because Zabetian does not use the SMTP and ESMTP protocols to authenticate the message and verify parameters relating to the message.

Claim 169

In claim 169, applicant recites that the first server maintains the electronic message and additionally provides a digital signature of the electronic message. There is also a recitation in claim 169 that the first server transmits the digital signature (the encrypted hash) of the electronic message from the first server to the sender at the time of the transmission of the electronic message from the first server to the sender. The mail

server 3 in Barkan does not perform these functions. It is certainly not disclosed in the abstract or on pages 8, 19 and 29 step c in Barkan. For example, Barkan does not disclose that the mail server 3 maintains the electronic message and additionally provides a digital signature of the electronic message. Since Barkan does not provide a digital signature of the message, the mail server 3 in Barkan does not transmit the digital signature to the user 1. Zabetian also does not disclose this information. Furthermore, claim 169 is allowable over the combination of Barkan and Zabetian because it is dependent from allowable claim 159 and for the reasons set forth in Sections III and V.

Claim 170

Claim 170 recites additional steps at the RPOST server (the first server in claim 170). For example, claim 170 recites that the first server transmits the electronic message to the sender after the transmission of the electronic message between the first server and the destination server. Claim 170 additionally recites that the first server disposes of the electronic message after the transmission of the electronic message by the first server to the sender but before the authentication of the message. The mail server 3 in Barkan does not dispose of the message after the transmission of the message to the user but before the authentication of the message. Zabetian does not dispose of the message and certainly does not dispose of the message before authentication of the message. As applicant has previously indicated, there is a significant difference between disposing of the message before authentication as in applicant's invention and as recited in claim 170 and disposing of the message after authentication as in Barkan. Furthermore, neither Zabetian nor Barkan discloses the step of using the selective one of the SMTP and

ESMTP protocols to authenticate the message and verify parameters relating to the message. Claim 170 is also allowable over the combination of Barkan and Zabetian because it is dependent from allowable claim 169 and for the reasons set forth in Sections III and V.

Barkan does not disclose the steps, recited in claim 171, of transmitting between the first server and the destination server the identity of the sender, the identity and address of the first server and the identity and address of the destination server at the time of the receipt of the electronic message by the first server and the time of the transmission to the first server from the destination server of the identity of the sender, the identity and address of the first server and the identity and address of the destination server. The mail server 3 in Barkan does not provide this information. Furthermore, pages 23, 30, 34 and 50 in Barkan do not disclose this information. Furthermore, there is no server in Zabetian that provides this information. This causes claim 171 to be allowable over the combination of Barkan and Zabetian. Claim 171 is also allowable over the combination of Barkan and Zabetian because it is dependent from allowable claim 170 and for the reasons specified in Sections III and V.

Claim 172

Claim 172 is dependent from claim 166 and is accordingly allowable over the combination of Barkan and Zabetian for the same reasons as claim 166. Claim 172 is also allowable over the combination of Barkan and Zabetian for the reasons set forth in Sections III and V.

Claim 173

Claim 173 is allowable over the combination of Barkan and Zabetian for a number of important reasons. Barkan does not disclose in the abstract and pages 8, 19 and 29 step c the step of receiving at the first server (the mail server 3 in Barkan) from the destination server (the user 1 in Barkan) an attachment including transmissions between the mail server 3 and the user 2 and relating to the message from the sender (the user 1 in Barkan). There is no disclosure in the abstract and on page 12 steps a, b, c; (c) pages 23, 24 step h, (d) page 30 step d and (e) page 33, first paragraph, of the step of transmitting from the first server (the mail server 3 in Barkan) to the sender (the user 1 in Barkan) the message and the attachments including the transmissions between the mail server 3 and the user 2. The intermediary 71 in Barkan is not a server and does not provide the message and the attachments to the user 1. No disclosure is further provided on pages 12 steps j-h, 29, 30, 31-32 and 34 in Barkan of the steps of transmitting from the sender (the user 1) to the first server (the mail server 3) the message and the attachment and authenticating the message on the basis of the message and the attachment. Barkan also does not disclose using the selected one of the SMTP and ESMTP protocols in the above steps. Zabetian also does not disclose the steps specified above. Contrary to the position of the Examiner, Zabetian does not even disclose the step of authenticating the message on the basis of the message, and the attachment including the transmission via the selected one of the SMTP and ESMTP protocols, received by the mail server 3 from the user 1. Claim 173 is also allowable over the combination of Barkan and Zabetian for the reasons set forth in Sections III and V.

Claim 174

Claim 174 recites that the attachment includes transmissions between servers intermediate the first server (the mail server 3 in Barkan) and the destination server (the user 2 in Barkan). According to the Examiner, Fig. 5 in Barkan shows an attachment including transmissions between servers intermediate the first server and the destination server. However, Fig. 5 in Barkan does not show the mail server 3 and the user 2. On that basis, applicant does not see how Fig. 5 in Barkan shows servers intermediate the first server (the mail server 3) and the destination server (the user 2). Claim 174 is also allowable over the combination of Barkan and Zabetian because of its dependency from claim 173 and for the reasons set forth in Sections III and V.

Claim 175

Since claim 175 is dependent from claim 173, it is allowable over the combination of Barkan and Zabetian for the same reasons as claim 173. Claim 175 is also allowable over the combination of Barkan and Zabetian for the reasons set forth in Sections III and V. Claim 175 is further allowable over Barkan because Barkan does not disclose the step of disposing of the message from the mail server 3 when the mail server 3 transmits to the user 1 the message and the attachment including the transmission between the mail server 3 and the user 2. Claim 175 is also allowable over Barkan because Barkan does not dispose of the message and the attachment, the disposition of the message and the attachment occurring before the authentication of the message and the attachment. Claim 175 is also allowable over Zabetian for the same reasons that it is allowable over Barkan. Claim 175 is additionally allowable over Zabetian because Zabetian does not disclose the

use of the SMTP and ESMTP protocols to authenticate the message and verify parameters relating to the message.

Claim 176

Claim 176 recites the following steps at the first server.

(1) receiving at the first server from the destination server the transmission of the identity of the sender, the identity and address of the first server and the identity and address of the destination server via the protocol selected from the group consisting of the SMTP protocol and the ESMTP protocol, and

(2) transmitting from the first server to the sender the identity of the sender, the identity and address of the first server and the identity and address of the destination server via the protocol selected from the group consisting of the SMTP protocol and the ESMTP protocol.

In claim 176, the first server is the RPOST server. The Examiner has cited pages 23 and 30 of Barkan against the first paragraph specified above. The first server in Barkan would probably be the mail server 3. Pages 23 and 30 in Barkan do not disclose the reception at the mail server 3 from the user 2 of the identity of the user 1, the identity and address of the mail server 3 and the identity and address of the user 2. The Examiner has cited pages 23, 30 and 34 against the second paragraph specified above. Pages 23, 30 and 34 in Barkan do not disclose any transmission from the mail server 3 to the user 1 of the identities and addresses of the user 1, the user 2 and the mail server 3. Zabetian also does not disclose the performance, at a server corresponding to the RPOST server, of the two (2) steps specified above. Actually, Zabetian does not even disclose the use of the

SMTP and the ESMTP protocols in an authentication or verification process. Claim 176 is also allowable over the combination of Barkan and Zabetian because it is dependent from allowable claim 173 and for the reasons specified in Sections III and V.

Claim 177

The Examiner has cited the abstract and pages 8, 19 and 29 step c against the step recited in claim 177 of providing at the first server digital signatures of the message and the attachment, including the transmission between the first server and the destination server relating to the message from the sender. The abstract and pages 8, 19 and 29 step c do not disclose any operation of the mail server 3 in performing the step specified above. The Examiner has also cited the abstract and page 12 steps a, b and c, pages 23-24 step h, page 30 step d and page 33 (first paragraph) against the step recited in claim 177 of transmitting from the first server to the sender the message and the attachment and the digital signatures of the message and the attachment. The abstract and pages 12 steps a, b and c, 23-24 step h, 30 step d and 33 (first paragraph) in Barkan do not disclose any operation of the mail server 3 in Barkan in performing this step. Furthermore, any operation of the mail server 3 in Barkan is encrypted. Zabetian also does not disclose any performance of these steps. Zabetian and Barkan additionally do not employ the SMTP protocol of the ESMTP protocol to authenticate a message or an attachment or to verify parameters relating to the message and the attachment. Claim 177 is also allowable over the combination of Barkan and Zabetian because of its dependency from allowable claim 173 and for the reasons set forth in Sections III and V.

Claim 178

The Examiner has cited the abstract and pages 12 steps a, b and c, 23-24 step h, 30 step d and 33 (first paragraph) against the step recited in claim 178 of transmitting from the first server to the sender the identity of the sender, the identity and address of the first server and the identity and address of the destination server at the time that the message and the transmissions between the first server and the destination server are transmitted form the first server to the sender. None of the citations from Barkan discloses such transmission from the mail server 3 to the user 1. There is also a citation by the Examiner of pages 23-24 steps j-h, 29, 30, 31-32 and 34 against the recitation in claim 178 that the sender transmits to the first server the information transmitted from the first server to the sender and that the first server authenticates the message on the basis of the information previously transmitted from the first sender to the sender and thereafter transmitted from the sender to the first server. There is no disclosure in the specified pages in Barkan that the user 1 transmits to the mail server 3 the information transmitted from the mail server 3 to the user 1 and that the mail server 3 authenticates this information. Actually, the mail server 3 in Barkan does not provide any authentication. Furthermore, any information transmitted by the mail server 3 in Barkan is encrypted. Additionally, Zabetian does not provide any authentication of any information transmitted to a server or any verification of any parameters relating to the authenticated information. Claim 168 is also allowable over the combination of Barkan and Zabetian because it is dependent from claim 166 and for the reasons specified in Sections III and V.

Claim 179

As with the other claims, claim 179 recites a series of steps that occur at the first server (the RPOST server). These steps provide for the operation of the first server in initially transmitting the message and related information from the sender to the destination server and subsequently from the destination server to the sender. The mail server 3 in Barkan does not operate initially to transmit the message and the related information to the user 2 and subsequently to transmit the message and the related information to the user 1. The mail server 3 operates only to indicate to the user 1 the encryption and decryption codes of the user 2 and to indicate to the user 2 the encryption and decryption codes of the user 1. The user 1 transmits the message (encrypted) to the user 2 rather than to the mail server 3. Because of this, Barkan cannot be applied to claim 179 to reject the claim. This may be further seen from the following:

a. The Examiner has cited the abstract and pages 23-24 step h and page 19 step b in Barkan against the step recited in claim 179 of receiving at the first server an electronic message from the sender for transmission of the message to the destination server. Barkan does not disclose in the cited pages that the mail server 3 receives an electronic message from the user 1 for transmission to the user 2. Zabetian also does not provide this disclosure.

b. The Examiner has cited the abstract and pages 12 steps a, b and c, 23-24 step h, and 30 step d in Barkan against the step recited in claim 179 of transmitting the electronic message from the first server to the

destination server. Barkan does not disclose in the cited pages that the mail server 3 transmits an electronic message to the user 2. Zabetian also does not provide this disclosure.

c. The Examiner has cited the abstract and pages 8, 19 and 29 step c in Barkan against the step recited in claim 179 that the first server receives transmissions between the first server and the destination server. However, Barkan does not disclose that the mail server 3 receives transmissions between the mail server 3 and the user 2. Zabetian also does not provide this disclosure.

d. The Examiner has cited the abstract and pages 12 steps a, b and c, 23-24 step h., 30 step d and 33 (first paragraph in Barkan against the step recited in claim 179 that the first server transmits to the sender the electronic message and at least a particular portion of the transmission between the first server and the destination server. Contrary to the position of the Examiner, Barkan does not disclose that the mail server 3 transmits to the user 1 an electronic message or at least a particular portion of a transmission between the mail server 3 and the user 2. Zabetian also does not provide this disclosure.

As will be seen from the above disclosure, neither Barkan nor Zabetian discloses any of the steps recited in claim 179. Because of this, Barkan and Zabetian cannot be combined to reject claim 179. Furthermore, Zabetian does not disclose the use of a selected one of the SMTP and ESMTP protocols to authenticate the message and verify

parameters relating to the message. Claim 179 is also allowable over the combination of Barkan and Zabetian for the reasons specified in Sections III and V.

Claim 180

Since claim 180 is dependent from allowable claim 179, claim 180 is allowable over the combination of Barkan and Zabetian for the same reasons as claim 179. Claim 180 is also allowable over Barkan because Barkan does not disclose that the electronic message and the at least particular portion of the transmission are provided by the sender to the first server and that the message is authenticated by the first server on the basis of the electronic message and the at least particular portion of the transmissions from the sender to the first server. The Examiner has cited the abstract and, pages 12 steps a, b and c, 23-24 step h, 30 step d and 33 (first paragraph) in Barkan against the recitation in claim 180. However, Barkan does not disclose that (a) the user 1 provides the message and the at least particular portion of the transmissions to the mail server 3 and (b) the mail server 3 authenticates the message. Zabetian also does not provide such disclosures. Furthermore, Zabetian does not disclose that the message is authenticated, and that related parameters are verified, in accordance with the selected one of the SMTP and ESMTP protocols. Claim 180 is also allowable over the combination of Barkan and Zabetian for the reasons set forth in Sections III and V.

Claim 181

The Examiner has rejected claim 181 as follows:

Pages 23, 30 and 34 in Barkan against the recitations in the claim. However, pages 23, 30 and 34 in Barkan do not relate to the recitations in claim 181 because:

(a) the first server (mail server 3) in Barkan does not maintain the electronic message and additionally provide a digital signature of the electronic message;

(b) the first server (the mail server 3) does not transmit the digital signature of the message to the sender (the user 1) with the message and the at least particular portion of the transmission between the first server (the mail server 3) and the destination server (the user 2); and

(c) the sender (the user 1) does not thereafter provide the digital signature to the first server (the mail server 3) with the electronic message and the at least particular portion of the transmission.

Further with respect to claim 181, the message in Barkan is encrypted rather than being unencrypted as in applicant's system. The mail server 3 in Barkan does not develop a digital signature of the message. The mail server 3 in Barkan does not transmit a digital signature of the message to the user 1 and the user 1 does not thereafter transmit the digital signature to the mail server 3. Claim 181 is allowable over Zabetian for the same reasons as it is allowable over Barkan. Furthermore, Zabetian does not use the selective one of the SMTP protocol and the ESMTP protocol to authenticate a message and verify parameters relating to the message. Claim 181 is also allowable over the

combination of Barkan and Zabetian because it is dependent from allowable claim 179 and for the reasons set forth in Section III and V.

Claim 182

The Examiner has cited page 33 of Barkan against the recitation in claim 182 that a digital signature of the electronic message and a digital signature of the electronic transmission are provided at the first server and transmitted to the sender with the electronic message and the electronic transmission. Page 33 in Barkan does not disclose that the mail server 3 in Barkan provides a digital signature of the electronic message and a digital signature of the electronic transmission. The Examiner has cited pages 23-24 steps j-h, 31-32 and 34 against the remainder of claim 182. Pages 23-24 steps j-h, 31-32 and 34 in Barkan do not disclose that the mail server 3 transmits the digital signature to the user 1 with the message and the at least particular portion of the transmission between the mail server 3 and the user 2. There is also no disclosure in these pages in Barkan that the user 1 thereafter provides the digital signature to the mail server 3 with the electronic message and the at least particular portion of the transmission. Claim 182 is allowable over Zabetian for the same reasons that it is allowable over Barkan. Claim 182 is also allowable over Zabetian because Zabetian does not disclose the use of a selective one of the SMTP and ESMTP protocols to authenticate a message and to verify parameters relating to the message. Claim 182 is additionally allowable over the combination of Barkan and Zabetian because it is dependent from allowable claim 180 and for the reasons set forth in Sections III and V.

Claim 183

Claim 183 is allowable over the combination of Barkan and Zabetian for a number of important reasons. The abstract and pages 23-24 step h and 19 step b in Barkan do not disclose the step of receiving at the mail server 3 an electronic message from the user 1 for transmission to the user 2. The abstract and pages 12 steps a, b and c, 23-24 step h and 30 step d in Barkan do not disclose the step of transmitting the message from the mail server 3 to the user 2. There is no disclosure in the abstract and pages 8, 19 and 29 step c of the step of receiving at the mail server 3 an electronic transmission between the mail server 3 and the user 2. No disclosure is provided in the abstract and pages 12 steps a, b and c, 23-24 step h, 30 step d and 33 (first paragraph) of Barkan of the step of transmitting from the mail server 3 to the user 1 the electronic message and the transmission between the mail server 3 and the user 2. Pages 23-24 steps j-h and 31-32 in Barkan do not disclose the step of receiving at the mail server 3 from the user 1 the electronic message and the electronic transmission between the mail server 3 and the user 2. As will be seen from the above, the electronic message and the electronic transmission are not disclosed in Barkan as being provided at the mail server 3. Because of this, Barkan cannot authenticate the electronic message at the mail server 3 on the basis of any electronic message transmitted by the mail server 3 to the user 1 and any electronic transmission received by the mail server 3 from the user 1. Claim 183 is also allowable over Zabetian for the same reasons as specified above for Barkan. Claim 183 is also allowable over Zabetian because Zabetian does not disclose the authentication of a message, and verification of parameters relating to the message, by using a selective one

of the SMTP and ESMTP protocols. Claim 183 is also allowable over the combination of Barkan and Zabetian for the reasons specified in Sections III and V.

Claim 187

Since claim 187 is dependent from claim 163, it is allowable over the combination of Barkan and Zabetian for the same reasons as claim 163. The Examiner has rejected claim 187 by applying the abstract and pages 12 steps a, b and c, 23-24 steps j-h, 30 step d and 33 (first paragraph) against the recitations in the claim. However, Barkan does not disclose that the user 1 transmits to the mail server 3 the electronic information transmitted from the mail server 3 to the user. Because of this, Barkan cannot disclose the step of authenticating the electronic message on the basis of the information transmitted from the user 1 to the mail server 3. Claim 187 is also allowable over Zabetian for the same reasons. Claim 187 is also allowable over Zabetian because Zabetian does not disclose the authentication of a message, and the verification of parameters relating to the message, by using a selected one of the SMTP and ESMTP protocols.

Claim 188

Like the other claims being actively prosecuted on this application, claim 188 recites steps that occur at the RPOST server. The Examiner has cited the abstract and pages 7, 8, 19 and 28 step c in Barkan against the first step recited in claim 188. However, the cited portions of Barkan do not disclose that the mail server 3 maintains the electronic message and additionally provides a digital signature of the electronic message and maintains the electronic attachment and additionally provides a digital signature of

the electronic attachment. The Examiner has cited the abstract and pages 12 steps a, b and c, 23-24 step h, 30 step d, 33 (1st paragraph) and 34 against the second step recited in claim 188. There is no disclosure in the cited portions of Barkan that the mail server 3 transmits the digital signature of the electronic message and the digital signature of the electronic attachment to the user 1 at the same time that the electronic message and the electronic attachment are transmitted by the mail server 3 to the user 1. Claim 188 is allowable over Zabetian for the same reasons that it is allowable over Barkan. Claim 188 is also allowable over Zabetian because Zabetian does not disclose the authentication of the message, and the verification of parameters relating to the message, by a selective one of the SMTP protocol and the ESMTP protocol. Claim 188 is additionally allowable over the combination of Barkan and Zabetian because it is dependent from allowable claim 163 and for the reasons specified in Sections III and V.

Claim 189

Claim 189 is dependent from claim 173 and is accordingly allowable over the combination of Barkan and Zabetian for the same reasons as claim 173. Claim 189 is also allowable over each of Barkan and Zabetian because neither reference discloses what is recited in the claim. For example, claim 189 is allowable over the abstract and pages 12 steps a, b and c, 23-24 step h, 30 step d, 33 (first paragraph) and 34 in Barkan because Barkan does not disclose that the mail server 3 maintains the electronic message and additionally provides a digital signature of the electronic message and maintains the electronic attachment and additionally provides a digital signature of the electronic attachment. Barkan also does not disclose that the mail server 3 transmits to the user 1

the electronic message and the electronic attachment and the digital signatures of the electronic message and the electronic attachment. Furthermore, neither Barkan nor Zabetian discloses electronic attachments. Neither reference also discloses the generation of digital signatures, whether from the electronic message or the electronic attachment. Furthermore, claim 189 is allowable over Zabetian because Zabetian does not employ the SMTP protocol or the ESMTP protocol to provide an authentication of a message or a verification of parameters relating to the message. Claim 189 is also allowable over the combination of Barkan and Zabetian for the reasons specified in Sections III and V.

Claim 190

The Examiner has cited the abstract and pages 12 steps a, b and c, 23-24 step h, 30 step d, 33 (first paragraph) and 34 in Barkan against the steps recited in claim 190. Claim 190 is allowable over Barkan for substantially the same reasons that claim 189 is allowable over Barkan. Claim 190 is also allowable over Zabetian for the same reasons that it is allowable over Barkan. Claim 190 is additionally allowable over Zabetian because Zabetian does not employ the SMTP protocol or the ESMTP protocol to provide an authentication of a message or a verification of parameters relating to the message. Claim 190 is also allowable over the combination of references because it is dependent from allowable claim 173 and for the reasons set forth in Sections III and V.

Claim 191

As previously indicated, the RPOST server sends the message to the destination address (the recipient). When the RPOST server has been informed that the message has reached the destination address, the RPOST server then maintains the message and

additionally provides a digital signature of the message. The RPOST server then sends a copy of the message and the digital signature of the message to the sender. The RPOST server also sends an attachment and the digital signature of the attachment to the sender. The attachment includes an indication of the servers between the RPOST server and the destination address. These servers are the intermediate stations through which the message has passed from the RPOST server to reach the destination address and through which the message has passed from the destination address to reach the RPOST server. The intermediate stations are indicated in accordance with the selected one of the SMTP and ESMTP protocols and their identities and addresses are recorded in an attachment.

Barkan provides an encrypted message instead of an unencrypted message. Barkan provides a mail server 3 to inform the user 1 (the sender) of the encrypted key of the user 2 (the recipient) and to inform the user 2 of the encrypted key of the user 1. The users 1 and 2 can then communicate with each other by having the user 1 use the user 2's key to communicate with the user 2 and by having the user 2 use the users 1's key to communicate with the user 1. The mail server 3 does not communicate a message from the user 1 to the user 2 and does not communicate a message from the user 2 to the user 1. Because of the above, Barkan does not disclose the steps recited in claim 191. Specifically, Barkan does not transmit from the user 1 to the mail server 3 the electronic message and the digital signature of the electronic message and the electronic attachment and the digital signature of the electronic attachment, including the transmission between the mail server 3 and the user 2. Since Barkan does not disclose the first step recited in claim 191, Barkan does not authenticate the message on the basis of the digital signatures

and the electronic message and the electronic attachment. Claim 191 is also allowable over Zabetian for the same reasons as discussed above with respect to Barkan. Claim 191 is also allowable over Zabetian because Zabetian does not use the SMTP and ESMTP protocols to authenticate the message and to verify the parameters relating to the message. Claim 191 is also allowable over the combination of Barkan and Zabetian because it is dependent from allowable claim 189 and for the reasons set forth in Sections III and V.

Claims 226-229

Claim 226 is an independent claim and claims 227-229 are dependent from claim 226. The Examiner has cited the same portion of Barton again each of claims 226-229. These portions are the abstract and pages 12 steps a, b and c, 23-24 step h, 30 step d and 34. Claims 226-229 are allowable over the cited portions of Barkan for the following reasons:

Claim 226

Barkan does not provide an electronic attachment transmitted between the mail server 3 (allegedly corresponding to the RPOST server) and the user 2 (the recipient). Furthermore, Barkan does not transmit the electronic attachment from the mail server 3 to the user 1 (the sender).

Claim 227

Barkan does not provide a digital signature (an encrypted hash) of the electronic attachment at the mail server 3. Barkan does not transmit the digital signature of the electronic attachment from the mail server 3 to the

user 1 at the time of transmitting the electronic attachment from the mail server 3 to the user 1.

Claim 228

The mail server 3 in Barkan does not receive the electronic attachment and the digital signature of the electronic attachment from the user 1. The mail server 3 does not authenticate the attachment at the mail server 3 on the basis of the electronic attachment and the digital signature of the electronic attachment.

Claim 229

The mail server 3 in Barkan does not receive the electronic attachment, and the digital signature of the electronic attachment, from the user 1. The mail server 3 in Barkan does not provide digital fingerprints (hashes) of the electronic attachment and the digital signature of the electronic attachment. Since the mail server 3 does not provide digital fingerprints as specified above, the mail server 3 cannot compare the digital fingerprints to authenticate the electronic attachment.

Claims 226- 299 are allowable over Zabetian for the same reasons as specified above for Barkan. Claims 226-229 are also allowable over Zabetian because Zabetian does not use the SMTP and ESMTP protocols to authenticate the message and verify parameters relating to the message. Claims 227-229 are additionally allowable over the combination of Barkan and Zabetian because they are dependent from allowable claims 226 and for the reasons specified in Sections III and V.

VIII. CONCLUSION

In the Office Action dated March 18, 2005, the Examiner rejected claims 115-121, 145-150, 159-183, 187-191 and 226-242 under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor, at the time the application was filed, had possession of the claimed invention. The problem apparently arose because applicant changed the word "message" in the claims to the term "unencrypted message." According to the Examiner in the Office Action dated March 18, 2005, the change to the term "unencrypted message" required "undue experimentation."

In Section II of the Remarks in this amendment, applicant has indicated that the terms "message" and "unencrypted message" have the same meaning but are distinguished significantly from an "encrypted message". On this basis, it should not have been necessary for applicant to amend the claims in order to avoid a rejection of the claims under 35 U.S.C. 112, first paragraph. However, to minimize the issues before the Examiner, applicant has amended the claims in order to eliminate from the claims the word "unencrypted" and the phrase "without any encryption" and the term "without encrypting the message". In making these changes, applicant has returned the language of the claims to essentially the wording at the time that the application was filed. However, applicant has clarified the language of the claims. The clarification in the language of the claims has not affected the scope of the claims. As a result, the scope of

the claims in this amendment is the same as the scope of the claims as originally filed and the scope of the claims in the previous amendment.

The Examiner did not object in the first Office Action to the language of the claims as originally filed in this application. Since the claims now in the application correspond substantially to the language in the claims as originally filed, applicant respectfully requests that the Examiner should enter applicant's proposed amendment to the claims.

In rejecting all of applicant's claims 115-121, 145-150, 159-183, 187-191 and 226-242, the Examiner has adopted global positions that are not supportable. For example, Barkan has disclosed nine (9) methods, each significantly different from the others. The Examiner has rejected applicant's claims by citing fragments of the nine (9) different methods in Barkan against the different steps recited in each single claim even though the fragments do not define a unitary and cohesive method. Applicant respectfully submits that each of applicant's claims should be allowed over Barkan since the different fragments cited in Barkan against the claim do not disclose a cohesive and unitary method.

Furthermore, the Examiner has applied Barkan against applicant's claims even though Barkan deals with an encrypted message and applicant's message is unencrypted. In applying Barkan against applicant's claims, the Examiner has disregarded the vast differences between Barkan and applicant's method that result from the unencrypted message in applicant's method and the encrypted message in Barkan. Furthermore, the Examiner has indicated in the Office Action dated March 18, 2005 that the difference

between a "message" and an "unencrypted message" is so great that it requires "undue experimentation." The Examiner has made this statement even though there is no difference between a "message" and an "unencrypted message". At the same time, the Examiner has treated a "message" as being the same as an "encrypted message" in rejecting applicant's claims on the basis of Barkan. The Examiner has adopted this position even though there is a vast difference between a "message" and an "encrypted message".

There is another significant difference between applicant and Barkan. In applicant's method, the RPOST server transmits the message between the sender and the destination address. In Barkan, the mail server 3 does not transmit the message between the user 1 and the user 2. In Barkan, the user 1 transfers the message to the user 2. The function of the mail server 3 in Barkan is to provide the user 1 with the user 2's encryption key and to provide the user 2 with the user 1's encryption key. In this way, the user 1 in Barkan can encrypt the message with the user 2's encryption key and transmit the encrypted message to the user 2 for decryption by the user 2. In like manner, the user 2 can encrypt the message with the user 1's encryption key and transmit the message to the user for decryption by the user 1.

Applicant processes an attachment in addition to processing the message. Applicant authenticates the attachment in addition to authenticating the message. By authenticating the attachment, applicant is ale to verify parameters related to the message. Barkan and Zabetian are not able to do this.

In spite of the unsupportable assumptions made by the Examiner, some of which are discussed in this Section VII, applicant's method is significantly different from Barkan in practically every step recited in every one of applicant's claims. This may be seen from applicant's analysis of the Examiner's position with respect to every step in every claim. Since applicant distinguishes patentably over Barkan in substantially every step recited in every claim, applicant's claims are allowable over Barkan. Applicant also distinguishes patentably over Zabetian in substantially every step recited in every claim in the same way as applicant distinguishes over Barkan. Because of this, Barkan and Zabetian cannot be combined to reject any of applicant's claims.

There is another significant difference between applicant and Zabetian. Applicant discloses and claims a system in which the SMTP and ESMTP protocols are provided for authenticating a message and for verifying parameters related to the message. Zabetian does not disclose a system in which the SMTP and ESMTP protocols are provided for authenticating a message and verifying parameters related to the message.

In view of the above, reconsideration and allowance of claims 115-121, 145-150, 159-183 and 226-242 are respectfully requested.

Respectfully submitted,
FULWIDER PATTON LEE & UTECHT, LLP

By: Ellsworth R. Roston
Ellsworth R. Roston
Registration No. 16,310

ERR:tlb
Encl. Return Postcard

Howard Hughes Center
6060 Civic Center Drive, Tenth Floor
Los Angeles, CA 90045
Telephone: (310) 824-5555
Facsimile: (310) 824-9696
Customer No. 24201